North Hill House School

E-Safety
Local Procedure
July 2024

Local Procedure Title	**E-Safety**
Service	**North Hill House School**
ACS Policy number and title	**ACS 38 E-Safety**
Local Procedure template reference	**ACS LP 38**
Local Procedure date	July 2024
Local Procedure review date	July 2026
Local Procedure Author(s)	Matt Davis/Carly Brown
Local Procedure Ratification	Checked and Approved by: Michael Pearce

1. Introduction

Technology is continuously evolving and has become integral to the lives of children and young people in today's society, both within schools and in their lives in the wider world.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Digital technology at North Hill House School (NHH) can promote discussion, creativity and increase awareness of context to provide positive learning experiences.

Children and young people have opportunities to use technology safely at NHH. The requirement to ensure that children and young people are able to use the internet and related technologies appropriately and safely is addressed as part of the wider duty of care which all staff at NHH are required to follow. This e-Safety policy should help to ensure safe and appropriate use.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher to the senior leaders and classroom teachers, support staff, parents, visitors, members of the community and the pupils at NHH.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing or distribution of personal images without consent
- Inappropriate communication or contact with others, including strangers online
- Cyber-bullying
- Access to unsuitable videos and online games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music, games or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and safeguarding policies).

Students at NHH have ASD and associated conditions and could be particularly vulnerable to negative experiences.

As with all other risks, it is impossible to completely eliminate those risks. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. This e-Safety policy how NHH intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. E-Safety Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Senior Leaders/Safeguarding Team:

- Senior Management/Safeguarding Team are responsible for ensuring the safety (including e-safety) of members of the school community, through the day-to-day responsibility for e-safety will be delegated to a suitable member of staff.
- Senior Management/Safeguarding Team/E-Safety Lead are responsible for ensuring that staff receive suitable CPD training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Senior Management/Safeguarding Team/E-Safety Lead will receive monitoring reports Aspris IT around issues that relate to e-Safety on the NHH School network.
- Senior Management/Safeguarding Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.

E-Safety Lead

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff.
- Liaise with school's technical team (Aspris IT).
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.
- Attends relevant meetings.

School Network Provider (Aspris IT):

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack as well as off-site access.
- That the school meets the e-safety technical requirements.
- That users may only access the school's networks through a properly enforced password protection policy.

- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current e-safety policy and procedures
- They have read, understood and signed the school 'Staff Acceptable User Policy'
- They report any suspected misuse or problem to the E-Safety Lead/Safeguarding Team
- Digital communications with pupils and parents should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, break/lunchtime clubs and extended schools activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and other digital devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. This is highly unlikely due to the school's filtering policy (Smoothwall) but any breach should be reported immediately to the E-Safety Lead/Safeguarding Team.

Designated Safeguarding Leads:

The Designated Safeguarding Leads (DSL/DDSLs) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- For incidents involving sharing of nudes, The DSL or equivalent should refer to the full 2024 guidance from the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, for managing incidents

Pupils:

- Are responsible for using the school ICT systems in accordance with the 'Pupil Acceptable Use Policy', which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones and other digital devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will therefore take opportunities to help parents understand these issues through supporting materials sent to parents/carers. Parents and carers will be responsible for:

- Endorsing the school policy on e-Safety.

3. Pupils taught to stay safe online

NHH uses a wide range of technology. This includes access to:

- Computers, laptops, iPads, tablets, cameras and other digital devices
- Internet which may include search engines and educational websites
- Email

Measures to mitigate these risks include:

- Teaching of ways to stay safe online based around curriculum guidance, in particular PSHE/ICT lessons but embedded in the whole curriculum across the school
- Ensuring that all NHH-owned devices are used in accordance with our acceptable use policies and with appropriate safety and security measures in place (such as Smoothwall)
- Ensuring that members of staff always evaluate websites, tools and apps fully before use in the classroom or recommending for use in homework
- Supervision of learners will be appropriate to their age and ability
- Student risk assessments updated to reflect any e-Safety issues they have encountered with measures in place to reduce future risks
- Ensuring the E-Safety of vulnerable students

Students at NHH have potential to be more at risk due to having Special Educational Needs and Disabilities (SEND) or mental health needs. NHH will ensure that differentiated and ability appropriate online safety education, access and support is provided to all students. When implementing an appropriate online safety policy and curriculum NHH will seek input from specialist staff as appropriate, including the E-Safety Lead.

4. Managing Access

Students in KS1, KS2 KS3 and KS4 will not have access to their mobile phones and other internet-enabled digital devices when onsite during the school day. They will only have access to these devices for longer school trips, with agreement from Senior Leadership.

Students are aware that they can use personal devices during the journey to school, which in many cases includes long taxi journeys. The devices are handed in to a named wallet for each student and kept safe in a box in a secured area. Students will be given their devices at the end of each school day when they have been called to go home and have exited the school building.

In any instance where a student is found to have brought a device into the school building, Senior Leadership will be notified immediately. Students are expected to hand the phone in. Where this does not happen, the student will be asked to go to the reception area where they are away from other students to mitigate the risk of e-Safety breaches.

Staff are aware that they are not permitted to use their own devices such as iPads or phones in the presence of students and must not take photos in school or on trips or show students content on these devices.

Students in Sixth Form (Year 12 and 13) are permitted use of their mobile phones and digital devices in school, but with the agreement that these are only to be used in the Sixth Form area. If they connect to the Aspris WiFi with their devices, they are under the same Smoothwall filtering system that other students and staff are.

5. Email

Staff will only email parents using their Aspris email address and will never use personal email addresses for such communication. Where students have been provided with NHH emails to support their education, staff will only use their Aspris email address for correspondence with the students, such as sending a worksheet or task to be completed electronically.

The email system enables students to communicate exclusively with teachers. Students are not able to email one another. While attachments are allowed, they may only include Microsoft Office applications such as Word, Excel, and PowerPoint. Additionally, students only have access to the email addresses of designated teachers in the Outlook address book.

Aspris IT require the following information to be incorporated into this policy which makes students aware of expectations they must agree and adhere to:

Monitoring

You should be aware that emails sent or received via Aspris email may be stopped and checked by IT for a variety of purposes, including, but not limited to, ensuring compliance with our internal policies and supporting internal investigations.

Emails and Cyber Security

The internet can be an unsafe place, so you should take care when using email against the cyber risks

You must be extremely careful when opening email attachments that are from senders that you do not know, as it may contain a computer virus that could harm your equipment.

You should be aware that senders you do not know may be trying to trick you so that they can steal your personal information, such as usernames, passwords and confidential information. Some emails may ask you to reply or complete and return an attachment. If this happens you must not do this and inform your teacher/tutor straight away.

Under no circumstances are you allowed to use your email in any illegal activity. The following activities are **strictly forbidden**, with no exceptions when using Aspris email:

(a) Aspris email must not be used to send or forward emails or documents containing harassing or offensive messages, including offensive comments against protected characteristics- race, gender, hair colour, disabilities, age, sexual orientation, religious

beliefs and practice, political beliefs, or national origin. If you receive any emails with this content from anyone, you should report the matter to your teacher/tutor straight away.

(b) You must not use your Aspris email to set up social media accounts, or purchase items online.
(c) You must not use another person's email account to send unwanted email messages or attempt to forge email messages or send email.
(d) You must not send chain letters or joke emails from your email account.
(e) You must not breach copyright or licensing laws when creating and sending emails or include attachments that contain software, music, digital photos, books or logos not belonging to you.
(f) You must not make false offers of products or services from your email account.
(g) You must not complete any form of monitoring which will stop emails intended for other email accounts.
(h) You must not send any kind of message to any other user in or outside of Aspris email system (for example, denial of service attack).
(i) You must not send information about your school/college staff or other Aspris staff or students to people in or outside of Aspris.
(j) You must not send unwanted email messages, including the sending of "junk mail" or other advertising material to individuals who did not request such material (email spam),
(k) You must not undertake or take part with others in any form of harassment via email as this is seen as Cyberbullying.

If you do not follow these rules, Aspris reserve the right to remove your email account.

6. Pupils' images and work on web

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. All staff are aware of specific children in school who do or do not have photograph permissions. If they do have permission, staff are aware of the platforms they can be used on.

Publishing students' images and work

All parents/carers will be asked upon entry to the school to give permission to use their child's work/photos in publicity materials or on the school website, Aspris Hub or Class Dojo. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/carers may withdraw or amend permission, in writing, at any time. Students' full names will not be published in association with their image and vice versa when published online.

Storage of Images

Images/films of children are stored securely on the school server where only NHH staff can access.

7. Social Networking

Social networking sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites in the school is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.

- All staff are advised not to have contact with parents and students on any social networking site.
- Students will be taught about legal ages for social networking sites and the dangers accompanied with using these, even at the correct age.

8. Cyberbullying

Online bullying and harassment via instant messaging, mobile phone texting, email, online gaming and chat rooms are potential problems that can have a serious effect on pupils both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk. NHH has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

- No access to mobile phones nor public chat rooms and Instant Messaging services on devices.
- Pupils are taught how to use the internet safely and responsibly and are given access to guidance and support resources from a variety of sources.
- Pupils are taught about the legal implications and potential consequences of engaging in activities that involve cyberbullying
- Specific education and training on cyberbullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) may be given as part of an annual Anti-Bullying Week and Safer Internet Day events.
- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with their teachers.
- Pupils are informed on how to report cyber bullying both directly within the platform they are on, and to school.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection and safeguarding procedures.

9. Monitoring and Filtering

NHH uses the Smoothwall filtering system. All Aspris devices used at NHH make use of Smoothwall which is set up by Aspris IT. This helps safeguard students from inappropriate websites or content, such as age-inappropriate online gaming, by blocking access to such sites. The E-Safety Lead and DSL have access to the Smoothwall Portal which enables them to further block and unblock sites and web pages if content is a breach of appropriate content is found.

When students or staff attempt to access content that is inappropriate, a notification is automatically sent immediately to the safeguarding team/E-Safety Lead with a note of the time, date, content that has been attempted to access, and reason that it has been filtered and blocked. The E-Safety Lead/DSL keep track of this through a spreadsheet which includes all students and staff, logging the Smoothwall notification alongside actions taken.

10. PREVENT

The counterterrorism and security bill was granted royal assent on 21 February 2015, which places a statutory duty on named organisations, including schools, to have due regard towards the need to prevent people being drawn into terrorism.

The most important part of this security bill is 'keeping pupils safe from the danger of radicalisation and extremism'.

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their message. The filtering systems used at NHH block inappropriate content, including extremist content. Where staff or pupils find unlocked extremist content, they must report it to the safeguarding team/E-Safety Lead.

Contents Checklist (Local Services may add additional items – this is a core list)			
Local responsibilities	✓	Risk assessments	✓
Contact plans	✓	Access to email	✓
Correspondence	✓	Access to social media	✓
Access to telephones	✓	Children and young people's own communication devices	✓
Record keeping	✓	'Local Rules' for safe and sensible communications and social media use	✓
Monitoring arrangements	✓		

Local Procedure Review History:

Date Reviewed	Reviewer	Summary of revisions
October 2024	Matt Davis	Additional links added for resources.
February 2025	Matt Davis	Included Emails section following Aspris IT rolling out student emails as a trial at NHH.
September 2025	Matt Davis	Wording change for Personal Development/PSHE.